Weierstrass半群とGoppa符号 (代数、言語のアルゴリズムと計算理論)

AUTHOR(S):

本間, 正明

CITATION:

本間, 正明. Weierstrass半群とGoppa符号 (代数、言語のアルゴリズムと計算理論). 数理解析研究所講究録 2008, 1604: 90-100

ISSUE DATE:

2008-06

URL:

http://hdl.handle.net/2433/139927

数理解析研究所講究録
第1604巻 2008年 90-100

Weierstrass 半群と Goppa 符号

Weierstrass semigroup and Goppa code

神奈川大学工学部　本間正明 (Masaaki HOMMA)*
Department of Mathematics, Faculty of engineering, Kanagawa University
homma@kanagawa-u.ac.jp

1 はじめに

研究集会では枝葉末節な事柄に多くの時間を割いてしまい，羊頭狗肉的講演となってしまった．本報告でその欠を補いたい[1]．したがって，講演での話題そのものに興味を持った故にこのページを開いて下さった方には失望を与える事になることをお詫びしたい．

本稿の構成は次の通り．2節では，話を進めるうえで最低限必要な「誤り訂正符号」についての知識をまとめる．3節では Goppa 符号とその最小距離の下からの評価について述べ，4節で Goppa 符号の中で1点符号とよばれるものについては gap 列や Weierstrass 半群を用いることにより最小距離の評価が精密化されることを説明する．最後の節で，2点符号の場合1点符号での諸結果に対応する事がどの程度解明されているかについて簡単に述べる．また，1点符号での諸結果に関連して，$\mathbb{N}_0$ の部分半群についてのある問題を提起する．

2 誤り訂正符号

この節では誤り訂正符号について，工学的意味を捨象して後段の解説に必要な事柄に絞って述べる．q を素数の正冪とし，$\mathbb{F}_q$ を q 個の元からなる有限体とする．n 次元座標空間 $(\mathbb{F}_q)^n$ の各ベクトル $\boldsymbol{v}$ に次のような「重み」を定める．

定義 2.1 $\boldsymbol{v}=(v_1,\ldots,v_n)\in(\mathbb{F}_q)^n$ について，$\mathrm{wt}(\boldsymbol{v})\overset{\mathrm{def}}{=}\#\{i\mid v_i\neq 0\}$ を $\boldsymbol{v}$ の **(Hamming) 重み**という．

容易に確認できるように，「重み」は

(i) $\mathrm{wt}(\boldsymbol{v})\geq 0$ かつ $\mathrm{wt}(\boldsymbol{v})=0\Leftrightarrow\boldsymbol{v}=\boldsymbol{0}$.

(ii) $\mathrm{wt}(\boldsymbol{v}+\boldsymbol{v}')\leq\mathrm{wt}(\boldsymbol{v})+\mathrm{wt}(\boldsymbol{v}')$

というノルムのような性質を持つ．したがって

定義 2.2 $\boldsymbol{v},\boldsymbol{v}'\in(\mathbb{F}_q)^n$ について，$\rho(\boldsymbol{v},\boldsymbol{v}')\overset{\mathrm{def}}{=}\mathrm{wt}(\boldsymbol{v}-\boldsymbol{v}')$ と定めると ρ は $(\mathbb{F}_q)^n$ の距離となる．この距離を **Hamming 距離**とよぶ．

*この研究は日本学術振興会科学研究費補助金 (基盤 C) (19540058) の援助を受けた．
[1]研究集会で講演の機会を与えて下さった米田二良教授に感謝します．

誤り訂正符号理論のある側面をきわめて単純化すれば

$((\mathbb{F}_q)^n, \rho)$ の部分空間の幾何

と言えなくもない．本稿での話題はこの側面に属する．

定義 2.3 C が $(\mathbb{F}_q)^n$ の $\mathbb{F}_q$-部分空間であるとき，C を **(線形) 符号**とよぶ．C が $[n,k,d]$-符号[2](あるいは，必要なら q 元体の意味で添え字 q を付け加えて $[n,k,d]_q$-符号) であるとは次の状況を意味する．

n は C を包む空間 $(\mathbb{F}_q)^n$ の次元，

$k = k(C) = \dim C$,

$d = d(C) = \min\{\rho(\boldsymbol{v},\boldsymbol{v}') \mid \boldsymbol{v},\boldsymbol{v}' \in C,\ \boldsymbol{v} \neq \boldsymbol{v}'\} = \min\{\mathrm{wt}(\boldsymbol{v}) \mid \boldsymbol{v} \in C \setminus \{\boldsymbol{0}\}\}$.

$d(C)$ を C の**最小距離** (あるいは，**最小重み**) とよぶ．

これら 2 つの量は当然ながら ρ-isometry な $(\mathbb{F}_q)^n$ の自己同型によって C を写しても変化しない．

工学上は n を固定したとき，k も d も共に大きい方が望ましいのだが，この 2 つの量は「あちらを立てればこちらが立たず」の関係にある．

補題 2.4 (Singleton bound) C を $[n,k,d]$-符号とする．このとき，$k + d \leq n + 1$.

実際，射影

$$\begin{array}{rcl} \pi : C \hookrightarrow (\mathbb{F}_q)^n & \to & (\mathbb{F}_q)^{n-(d-1)} \\ (v_1,\ldots,v_{n-(d-1)},\ldots,v_n) & \mapsto & (v_1,\ldots,v_{n-(d-1)}) \end{array}$$

を考えるとき，$\ker(\pi)$ の元は第 1 座標から第 $n-(d-1)$ 座標までは 0 : $(0,\ldots,0,\overbrace{*,\ldots *}^{d-1})$. 最小重み $d(C) = d$ であるから，残りの位置 $*$ も全て 0. すなわち，π は injective であるから，$\dim C \leq \dim(\mathbb{F}_q)^{n-(d-1)}$.

定義 2.5 $(\mathbb{F}_q)^n$ 上の 2 次形式

$$(\mathbb{F}_q)^n \times (\mathbb{F}_q)^n \ni ((x_1,\ldots,x_n),(y_1,\ldots,y_n)) \mapsto \sum_{i=1}^{n} x_i y_i \in (\mathbb{F}_q)^n$$

は明らかに非退化であるが，この非退化 2 次形式による $[n,k]$-符号 C の双対空間を $C^\perp$ と表す．これは，明らかに $[n,n-k]$-符号である．$C^\perp$ を C の**双対符号**という．

定義から $(C^\perp)^\perp = C$ であるので，$C^\perp$ の基底を一組とり，これらを行ベクトルとする $(n-k)\times n$ 行列 H を考えると，C は連立方程式 $H\,{}^t(x_1,\ldots,x_n) = {}^t(0,\ldots,0)$ の解空間である．したがって

$$d(C) = \min\{s \in \mathbb{N} \mid H \text{ のある } s \text{ 個の列ベクトルは 1 次従属 }\}$$

である．これによれば，符号 C の構成が具体的に与えられたとき，その最小距離 $d(C)$ を求めることはさほど困難でないようにも思えるが，多くの場合，それほど容易なことではない．

本稿の主題も，代数曲線を用いて構成された符号の最小距離がどのように下から評価できるかということに関わっている．

[2] d を明示する必要がない，あるいは d の値が不明であるというような状況では $[n,k]$-符号ということもある．

3 Goppa符号

代数曲線の定義を述べその性質をいくつか説明するだけで，それなりの頁数を費やすことになるので，ここでは例をひとつ考え，それに即していくつかの概念を説明する．

例 3.1 3^2 元体 $\mathbb{F}_{3^2}$ 上の射影平面 $\mathbb{P}^2$ の斉次座標を X, Y, Z とする．方程式

$$Y^3Z + YZ^3 = X^4 \tag{1}$$

を満たす $\mathbb{F}_{3^2}$ の代数的閉包 K に座標を持つような点全体 $\mathcal{X}$ は代数曲線とよばれるひとつの対象である．

いま $x = \frac{X}{Z}$，$y = \frac{Y}{Z}$ と置くとこれらは，$\mathcal{X}$ 上で点の斉次座標の表示の仕方に依存しない (極を持つ) 関数となる．明らかに x と y の間には

$$y^3 + y = x^4 \tag{2}$$

という関係式が成り立つ．これを $\mathcal{X}$ のアフィン方程式という．

言い換えれば，関数 x, y とは，$\tilde{x}, \tilde{y}$ を不定元として，多項式環の剰余環 $\mathbb{F}_{3^2}[\tilde{x}, \tilde{y}]/(\tilde{y}^3 + \tilde{y} - \tilde{x}^4)$ における $\tilde{x}, \tilde{y}$ の像と見る事もできる．関数の和，差，積も，定数も含めて，関数と考えるのが普通であろうから，$\mathbb{F}_{3^2}[x, y] = \mathbb{F}_{3^2}[\tilde{x}, \tilde{y}]/(\tilde{y}^3 + \tilde{y} - \tilde{x}^4)$ のどの元も自然に関数と考えうる．$\tilde{y}^3 + \tilde{y} - \tilde{x}^4$ は (絶対) 既約であるから $\mathbb{F}_{3^2}[x, y]$ は整域．その商体 $\mathbb{F}_{3^2}(x, y)$ の元も $\mathcal{X}$ 上の関数と見る事ができる．この体を $\mathcal{X}$ の関数体とよび，$\mathbb{F}_{3^2}(\mathcal{X})$ と表す．これらの事柄は $\mathbb{F}_{3^2}$ の代数的閉包 K で考えても同様に進行するので，K 上の関数体 $K(\mathcal{X})$ も自然に考えうる．$K(\mathcal{X}) = K \cdot \mathbb{F}_{3^2}(\mathcal{X})$ である．

$\mathcal{X}$ 上の点で座標がすべて $\mathbb{F}_{3^2}$ の元で取れるような点を $\mathbb{F}_{3^2}$-有理点とよぶ．$\mathcal{X}$ 上の $\mathbb{F}_{3^2}$-有理点全体をやや紛らわしい記号であるが $\mathcal{X}(\mathbb{F}_{3^2})$ で表す．

$\mathcal{X}(\mathbb{F}_{3^2})$ を具体的に記述して見る．$t^2 + 1$ は $\mathbb{F}_3 = \{0, 1, -1\}$ 上既約であるので，$t^2 + 1 = 0$ の根の一方を η として，$\mathbb{F}_{3^2} = \mathbb{F}_3[\eta]$ である．$\mathbb{P}^2$ の中で，直線 $Z = 0$ と 曲線 (1) との交点は $(0, 1, 0)$ のみである．この点を P_∞ で表す．$\mathcal{X}(\mathbb{F}_{3^2}) \setminus \{P_\infty\}$ の各点は $(\alpha, \beta, 1)$ (ここで，(α, β) は (2) を満たす) という形であるからアフィン座標 (α, β) を用いて $P_{\alpha,\beta}$ という書き方をする．このとき，直接計算することにより，

$$\begin{aligned}
\mathcal{X}(\mathbb{F}_{3^2}) \setminus \{P_\infty\} &= \{P_{0,0}, P_{0,\eta}, P_{0,-\eta}\} \\
&\cup \{P_{\alpha,\beta} \mid \alpha = 1, -1, \eta, -\eta;\ \beta = -1, -1+\eta, -1-\eta\} \\
&\cup \{P_{\alpha,\beta} \mid \alpha = 1+\eta, 1-\eta, -1+\eta, -1-\eta;\ \beta = 1, 1+\eta, 1-\eta\}
\end{aligned}$$

となることが分かる．

$\mathcal{X}$ の各点 Q について，$\mathcal{O}_Q = \{f \in K(\mathcal{X}) \mid f \text{ は } Q \text{ において有限値をとる}\}$ は離散付値環となり，$K(\mathcal{X})$ はこの付値 v_Q により付値体となる．$f \in K(\mathcal{X})$ について，f の因子[3]を $\operatorname{div} f = \sum_{Q \in \mathcal{X}} v_Q(f) Q$ によって定める．例えば，

$$\operatorname{div} x = P_{0,0} + P_{0,\eta} + P_{0,-\eta} - 3P_\infty, \quad \operatorname{div} y = 4P_{0,0} - 4P_\infty$$

である．

---

[3] $\mathcal{X}$ の点どもから形式的に生成される自由アーベル群の元を因子とよぶ．すなわち，因子 D とは $D = \sum_{Q \in \mathcal{X}} m_Q Q$ ($m_Q \in \mathbb{Z}$) で，有限個の $Q \in \mathcal{X}$ を除いて $m_Q = 0$ となるようなものである．$\{Q \mid m_Q \neq 0\}$ を D の support という．2 つの因子 $D = \sum_{Q \in \mathcal{X}} m_Q Q$, $E = \sum_{Q \in \mathcal{X}} n_Q Q$ がすべての $Q \in \mathcal{X}$ について $m_Q \geq n_Q$ となっている状況を $D \succ E$ と書く．

$f \in \mathbb{F}_{3^2}(\mathcal{X})^*$ について，記号 df を考え，$\{df \mid f \in \mathbb{F}_{3^2}(\mathcal{X})^*\}$ を基底とする $\mathbb{F}_{3^2}(\mathcal{X})$-ベクトル空間の，通常の微分規則 (i) 作用 d の $\mathbb{F}_{3^2}$-線形性，(ii) $f \in \mathbb{F}_{3^2} \Rightarrow df = 0$，(iii) $d(fg) = fdg + gdf$ で生成される部分空間を法として商空間をとったものの元を微分とよぶ．これは $\mathbb{F}_{3^2}(\mathcal{X})$-ベクトル空間として 1 次元である．この空間を $\Omega_{\mathbb{F}_{3^2}(\mathcal{X})/\mathbb{F}_{3^2}}$ で表す．同様にして，K 上の微分の空間 $\Omega_{K(\mathcal{X})/K}$ も考えられる．また，標数が 3 であるので，微分規則 (iii) により，$df^3 = 0$ となる．

$\omega \in \Omega_{K(\mathcal{X})/K}$ について $\operatorname{div}\omega$ を次のように定める：各点 $Q \in \mathcal{X}$ について $v_Q(t_Q) = 1$ となる $t_Q \in K(\mathcal{X})$ を選んでおく[4]．dt_Q は $\Omega_{\mathcal{X}/K}$ の元としては 0 ではないので，$\dim_{K(\mathcal{X})} \Omega_{K(\mathcal{X})/K} = 1$ より，ある $f \in K(\mathcal{X})$ が存在して $\omega = f dt_Q$ と書ける．この f を $\frac{\omega}{dt_Q}$ と書くことにして $\operatorname{div}\omega = \sum_{Q \in \mathcal{X}} v_Q(\frac{\omega}{dt_Q})Q$ によって定める．

dx と dy との関係を見てみる．(2) の両辺に d を作用させ微分規則を用いると，左辺は $d(y^3+y) = dy$，右辺は $dx^4 = 4x^3dx = x^3dx$ $(4 = 1\,!)$．ゆえ，$dy = x^3dx$ である．$\operatorname{div} dx = 4P_\infty$ が分かる[5]ので $\operatorname{div} dy = 3\operatorname{div} x + \operatorname{div} dx = 3P_{0,0} + 3P_{0,\eta} + 3P_{0,-\eta} - 5P_\infty$ である．　[例 3.1 終わり]

状況設定 3.2 有限体 $\mathbb{F}_q$ 上定義された特異点を持たない代数曲線 $\mathcal{X}$ の上で，$\mathbb{F}_q$-有理因子[6] G と，G の support に含まれない相異なる $\mathbb{F}_q$-有理点 $P_1, \ldots, P_n$ を考える．便宜上 $D = P_1 + \cdots + P_n$ と因子の記号を用いる．上の例のように，$\mathbb{F}_q(\mathcal{X})$ を $\mathcal{X}$ の $\mathbb{F}_q$ 上の代数関数体，$\Omega_{\mathbb{F}_q(\mathcal{X})/\mathbb{F}_q}$ を $\mathbb{F}_q(\mathcal{X})$ の $\mathbb{F}_q$ 上の微分加群とする．つぎの 2 つの $\mathbb{F}_q$ ベクトル空間を考える：

$$L(G) = \{f \in \mathbb{F}_q(\mathcal{X}) \mid \operatorname{div} f + G \succ 0\} \cup \{0\} \tag{3}$$

$$\Omega(G - D) = \{\omega \in \Omega_{\mathbb{F}_q(\mathcal{X})/\mathbb{F}_q} \mid \operatorname{div}\omega \succ (G - D)\} \cup \{0\} \tag{4}$$

例 3.3 (例 3.1 の続き) 付値環 $\mathcal{O}_Q$ の極大イデアルはその local parameter $t = t_Q$ で生成され，この付値による完備化は $K[[t]]$ である．したがって，$K(\mathcal{X}) \subset K((t))$ である．$\omega \in \Omega_{K(\mathcal{X})/K}$ について $\frac{\omega}{dt}$ を上の包含関係で $K((t))$ の元と見ることにより $\omega = (\sum_\nu a_\nu t^\nu)dt$ $(a_\nu \in K)$ と書けるが，ω の Q に於ける留数を $\operatorname{res}_Q \omega = a_{-1}$ によって定める[7]．

$z = \prod_{\alpha \in \mathbb{F}_{3^2}} (x - \alpha)$ とすると，

$$\operatorname{div} z = \sum_{\substack{(\alpha,\beta) \in (\mathbb{F}_{3^2})^2 \\ \beta^3 + \beta = \alpha^4}} P_{\alpha,\beta} - 27P_\infty$$

である．$\omega_0 = \frac{dx}{z}$ を考えると

$$\operatorname{div}\omega_0 = 31P_\infty - \sum_{\substack{(\alpha,\beta) \in (\mathbb{F}_{3^2})^2 \\ \beta^3 + \beta = \alpha^4}} P_{\alpha,\beta}$$

となり，ω_0 は $\mathcal{X}(\mathbb{F}_{3^2}) \setminus \{P_\infty\}$ の各点 $P_{\alpha,\beta}$ で 1 位の極を持つ．さらに，点 $P_{\alpha,\beta}$ での local parameter として $x - \alpha$ がとれることを考えれば，$\operatorname{res}_{P_{\alpha,\beta}} \omega_0 = 1/\prod_{\gamma \in \mathbb{F}_{3^2} \setminus \{\alpha\}} (\alpha - \gamma) = -1$ である．

---

[4] このような t_Q を $\mathcal{X}$ の Q に於ける local parameter という．

[5] これを説明するにはもう少し準備が必要なので，ここでは省略する．

[6] $\mathcal{X}$ には自然に q 乗 Frobenius 写像 F_q が作用している．例 3.1 の場合には $(X, Y, Z) \mapsto (X^{3^2}, Y^{3^2}, Z^{3^2})$ を考える事に相当する．$Q \in \mathcal{X}$ について，それが $\mathbb{F}_q$-有理点である条件は $F_q(Q) = Q$ であるが，因子についても $F_q(D) = D$ (support の点自体は動いても良い) となるとき，$\mathbb{F}_q$-有理であるという．

[7] $a_\nu \in K$ は当然 local parameter t のとり方に依存するが，a_{-1} だけは，Q における別の local parameter に取り替えても不変である．

定義 3.4 (Ω-構成法) 状況設定 3.2 の下で $\mathbb{F}_q$ ベクトル空間 (4) を用いて

$$\begin{array}{rccc} \mathrm{res}: & \Omega(G-D) & \to & (\mathbb{F}_q)^n \\ & \omega & \mapsto & (\mathrm{res}_{P_1}(\omega),\ldots,\mathrm{rcs}_{P_n}(\omega)) \end{array}$$

という線形写像を考える．ただし，$\mathrm{res}_{P_i}(\omega)$ は微分 ω の P_i での留数である．この写像による像 $C_\Omega(D,G) \stackrel{\mathrm{def}}{=} \mathrm{res}(\Omega(G-D))$ は $(\mathbb{F}_q)^n$ 内の符号である．これを Ω-構成法とよぶ．

定義 3.5 (L-構成法) 状況設定 3.2 の下で $\mathbb{F}_q$ ベクトル空間 (3) を用いて

$$\begin{array}{rccc} \mathrm{ev}: & L(G) & \to & (\mathbb{F}_q)^n \\ & f & \mapsto & (f(P_1),\ldots,f(P_n)) \end{array}$$

という線形写像を考えれば，その像 $C_L(D,G)$ これを L-構成法とよぶ．

以上の符号を総称して **Goppa 符号** (あるいは，**代数曲線符号**) とよぶ．この定義から代数曲線の初歩的知識[8]により，それらの次元 k および最小距離 d の下からの評価を与えることができる．(詳しい議論は例えば [16] を参照のこと.)

状況設定 3.6 以下，状況設定 3.2 の代数曲線 $\mathcal{X}$ の genus を g とする．(genus の定義は脚注 8 を参照．)

定義と上に説明したことから直ちに

補題 3.7 状況設定 3.2, 3.6 の下で

(a) $C_\Omega(D,G)$ について，

$$k(C_\Omega(D,G)) = i(G-D) - i(G);\quad d(C_\Omega(D,G)) \geq \deg G - (2g-2).$$

(b) $C_L(D,G)$ について，

$$k(C_L(D,G)) = l(G) - l(G-D);\quad d(C_L(D,G)) \geq n - \deg G.$$

が分かる．($l(*)$, $i(*)$ の定義は脚注 8 を参照のこと.)
これを，もう少し具合の良い場合だけに限ると

補題 3.8 状況設定 3.2, 3.6 の下で，さらに $2g-2 < \deg G < n$ とする．このとき，

(a) $C_\Omega(D,G)$ について，

$$k(C_\Omega(D,G)) = n + g - \deg G - 1;\quad d(C_\Omega(D,G)) \geq \deg G - (2g-2).$$

(b) $C_L(D,G)$ について，

$$k(C_L(D,G)) = \deg G + 1 - g;\quad d(C_L(D,G)) \geq n - \deg G.$$

---

[8] $E = \sum_{\nu=1}^{s} m_\nu Q_\nu$ を $\mathcal{X}$ 上の因子とするとき，E の次数 $\deg E$ を $\sum_{\nu=1}^{s} m_\nu$ で定める．さらに $L(E) = \{f \in \mathrm{F}_q(\mathcal{X}) \mid \mathrm{div}\, f + E \succ 0\} \cup \{0\}$, $\Omega(E) = \{\omega \in \Omega_{\mathbb{F}_q(\mathcal{X})/\mathbb{F}_q} \mid \mathrm{div}\,\omega \succ E\} \cup \{0\}$ とし $l(E) = \dim L(E)$, $i(E) = \dim \Omega(E)$ と書く．$i(0)$ を $\mathcal{X}$ の genus とよび，g で表す．このとき，Riemann-Roch の等式 $l(E) = \deg E + 1 - g + i(E)$ が成り立つ．また，関数 f については $\deg(\mathrm{div}\, f) = 0$, であり，微分 ω については $\deg(\mathrm{div}\,\omega) = 2g-2$ であるので，$\deg E < 0$ ならば $l(E) = 0$ であり，$\deg E > 2g-2$ ならば $i(E) = 0$ である．

となる.

定義 3.9 上で述べた $d(C_L(D,G))$ の下界 $n-\deg G$ を $C_L(D,G)$ の**設計距離**とよび，$d(C_\Omega(D,G))$ の下界 $\deg G-(2g-2)$ を $C_\Omega(D,G)$ の**設計距離**とよぶ.

与えられた Goppa 符号の真の最小距離が設計距離をどの程度上回るかを見ることは[9]，符号の良し悪しを考えるひとつの視点である．次の節でそのような視点からの結果を紹介する.

また留数定理[10]から次の duality が成り立つことが分かる.

補題 3.10 $C_L(D,G)$ と $C_\Omega(D,G)$ とは互いに双対符号である.

なお，状況設定 3.2 の下で，上手に G' をとると $C_\Omega(D,G)=C_L(D,G')$ と，単に ρ-isometry ではなく真に等しくなる．したがって Goppa 符号を考えるとき L-構成法と Ω-構成法とは単に表現の仕方の違いにすぎない[11].

4 Weierstrass 半群と gap 列

この節では特異点を持たない代数曲線 $\mathcal{X}$ 上の点 Q における "Weierstrass 半群" と "gap 列" について説明する.

定義 4.1 $WS(Q):=\left\{m\in\mathbb{N}_0 \middle|\ \begin{array}{l}\text{ある } f\in K(\mathcal{X}) \text{ で } Q \text{ だけに極を持ち，}\\ \text{極位数が } m \text{ となるようなものが存在する．}\end{array}\right\}$ とする[12]．$WS(Q)$ は明らかに，加法について半群をなす．この半群を Q における **Weierstrass 半群**とよぶ.

また，$\mathcal{X}$ が $\mathbb{F}_q$ 上定義されているとき，$P\in\mathcal{X}(\mathbb{F}_q)$ について

$$WS_{\mathbb{F}_q}(P):=\left\{m\in\mathbb{N}_0 \middle|\ \begin{array}{l}\text{ある } f\in\mathbb{F}_q(\mathcal{X}) \text{ で } P \text{ だけに極を持ち，}\\ \text{極位数が } m \text{ となるようなものが存在する．}\end{array}\right\}$$

を考えることができるが，$WS_{\mathbb{F}_q}(P)=WS(P)$ である.

g を曲線 $\mathcal{X}$ の genus とする．$\mathbb{N}_0\setminus WS(Q)$ は g 個の数からなる有限集合であるが，これら g 個の数を小さい順に並べたものを Q における **gap 列**とよぶ.

例 4.2 (例 3.1, 3.3 の続き) $\mathcal{X}$ を例 3.1 での曲線とする.

$$\{f\in\mathbb{F}_q(\mathcal{X})\mid f \text{ は高々} P_\infty \text{だけに極を持つ}\}=\cup_{\nu=0}^{\infty}L(\nu P_\infty)=\mathbb{F}_q[x,y]$$

であり，x の P_∞ における極位数は 3，y のそれは 4 であるので，P_∞ における Weierstrass 半群の元を，3 を法として並べると

$$WS(P_\infty)=\left\{\begin{array}{ccc}0 & & \\ 3 & 4 & \\ 6 & 7 & 8\\ 9 & 10 & 11\\ \vdots & \vdots & \vdots\end{array}\right\}$$

---

[9] このような研究方向を，熟さない言葉であるが，後の引用の為に「最小距離評価の改善」と呼ぶことにする.

[10] $\omega\in\Omega_{K(\mathcal{X})/K}$ について，$\sum_{P\in\mathcal{X}}\mathrm{res}_P\omega=0$.

[11] とは言うものの実際の取り扱い上は「単に表現の仕方の違い」では済まされない相違が生じることも多い．例えば，次節以降で 1 点符号なるものを扱うが，Ω-構成法による 1 点符号が L-構成法による 1 点符号で表現される保証は一般にはない.

[12] $\mathbb{N}_0$ は非負整数全体を意味する.

となる．上の空白部分 $\{1,2,5\}$ が P_∞ における gap 列をなす．

再び状況設定 3.2, 3.6 の下，Goppa 符号 $C_L(D,G)$, $C_\Omega(D,G)$ に立ち返る．

定義 4.3 $\mathcal{X}$ の $\mathbb{F}_q$-有理点を 2 組に分け，$\mathcal{X}(\mathbb{F}_q) = \{P_1,\ldots,P_m\} \cup \{Q_1,\ldots,Q_n\}$ とし，$G = \nu_1 P_1 + \cdots + \nu_m P_m$ $(\nu_1,\ldots,\nu_m \in \mathbb{N}_0)$，$D = Q_1 + \cdots + Q_n$ と選んだとき，$C_L(D,G)$, $C_\Omega(D,G)$ を m 点符号とよぶ．

以下しばらくは 1 点符号を扱い，G の support となる点を P_∞ で表す．
gap 列を「最小距離評価の改善」(脚注 9) に用いたのは Garcia and Lax [3] をもって嚆矢とする．

定理 4.4 (Garcia - Lax) α, β を共に P_∞ における *gap* とする．$G = (\alpha+\beta-1)P_\infty$ であるとき，

$$d(C_\Omega(D,G)) \geq \alpha+\beta-(2g-2)$$

である．

注意：定理 4.4 の評価式の右辺は $\deg G-(2g-2)+1$ であるので，設計距離より 1 だけ改善されている．
その後，S. J. Kim を加えた Garcia, Kim and Lax[4] でこれを一般化した．

定理 4.5 (Garcia - Kim - Lax) t を自然数とする．α, β は共に P_∞ における *gap* で $\alpha+t \leq \beta$ を満たし $\alpha, \alpha+1, \ldots \alpha+t$ および $\beta-(t-1), \beta-(t-2), \ldots, \beta$ をそれぞれ引き続く $t+1$ 個と t 個の *gaps* の列とする．$G = (\alpha+\beta-1)P_\infty$ ならば

$$d(C_\Omega(D,G)) \geq \alpha+\beta+t-(2g-2)$$

となる．

注意：定理 4.5 の評価式の右辺は $\deg G-(2g-2)+t+1$ であるので，設計距離より $t+1$ だけ改善されている．

5 Weierstrass 半群の性質による 1 点符号の最小距離の評価

1998 年に Heijnen and Pellikaan [5] は Feng and Rao [2] の Goppa 符号の復号法から着想を得て Weierstrass 半群の性質によって，1 点符号の最小距離の評価を与えた．以下にこの概要を説明する．前節後半に引き続き，状況設定 3.2, 3.6 の下で $G = lP_\infty$ として 1 点符号 $C_\Omega(D,G)$ を考える．

状況設定 5.1 $P_\infty \in \mathcal{X}$ における Weierstrass 半群の元を小さい順に並べたものを $\{0 = \rho_1 < \rho_2 < \ldots\}$ とする．$C_L(D,\rho_1 P_\infty) \subseteq C_L(D,\rho_2 P_\infty) \subseteq \cdots$ であるが，十分大きな ρ_k については $C_L(D,\rho_k P_\infty) = (\mathbb{F}_q)^n$ (全体空間) となる．このような，最初の値を M とする．したがって，補題 3.10 により，

$$C_\Omega(D,\rho_1 P_\infty) \supseteq C_\Omega(D,\rho_2 P_\infty) \supseteq \cdots \supset C_\Omega(D,MP_\infty) = (0)$$

となる．

定義 5.2 $\rho_l < M$ となるような l について，

$$a(l) = {}^{\#}\{\rho_i \mid \text{ある } \rho_j \text{ が存在して } \rho_i + \rho_j = \rho_{l+1}\ \}$$

とする[13]．さらに，

$$b(l) = \min\{a(l') \mid \rho_l \leq \rho_{l'} < M \text{ かつ } C_\Omega(D, \rho_{l'}P_\infty) \neq C_\Omega(D, \rho_{l'+1}P_\infty)\}$$

とする．

定理 5.3 (Heijnen-Pellikaan) $C_\Omega(D, \rho_l P_\infty) \geq b(l)$.

上の評価を **order bound** とよぶ．

例 5.4 例 4.2 で考えた Weierstrass 半群については $\rho_1 = 0, \rho_2 = 3, \rho_3 = 4, \rho_l = l+2\ (l \geq 4)$ である．さらに，$M = 32 = \rho_{30}$ となる．これらについて，$a(l)$ を直接計算して見れば，$a(1) = 2, a(2) = 2, a(3) = 3, a(4) = 4, a(5) = 3, a(6) = 4, a(7) = 6, a(8) = 6, a(9) = 7, a(l) = l - 2\ (10 \leq l \leq 29)$ となる．

例 3.1 の曲線は次の状況の特殊な場合であった．

定義 5.5 有限体 $\mathbb{F}_q$ として，q が素数冪の平方とする．つまり，$\sqrt{q}$ は整数である．このとき平面曲線

$$\mathcal{H}_{\sqrt{q}}:\ Y^{\sqrt{q}}Z + YZ^{\sqrt{q}} = X^{\sqrt{q}+1} \tag{5}$$

を $\mathbb{F}_q$ 上で考えたものを **Hermitian** 曲線とよぶ．

(5) と直線 $Z = 0$ との交点は曲線 (1) の場合と同じく $(0:1:0)$ だけであり，この点を P_∞ で表し，他の点は $x = \frac{X}{Z}, y = \frac{Y}{Z}$ に関するアフィン座標で表示する．Hermitian 曲線は絶対既約でその genus は $\frac{1}{2}\sqrt{q}(\sqrt{q}-1)$ であり，同じ genus を持つ $\mathbb{F}_q$-曲線の中では最大の有理点の個数 $(\sqrt{q})^3 + 1$ を到達する．また定義式が扱いやすい形であることも相俟って Goppa 符号の発見以来多くの著作のなかで好んで例として取り上げられてきた．またこの曲線は比較的大きな automorphism group を持ち，それは $\mathcal{H}_{\sqrt{q}}(\mathbb{F}_q)$ に 2 重可遷に作用する[14]．したがって，この曲線上で 1 点符号や 2 点符号を考えるときは，どの 1 点ないし 2 点を選んでもよい．

Hermitian 曲線上の 1 点符号すべてについて，それらの最小距離 $d(C_L(D, mP_\infty))$ を完全に決定したのは Yang and Kumar [18] であった (1992 年)．Hermitian 曲線上では

$$C_\Omega(D, mP_\infty) = C_L(D, ((\sqrt{q})^3 + q - \sqrt{q} - 2 - m)P_\infty) \tag{6}$$

であるので，$d(C_\Omega(D, mP_\infty))$ についても決着したことになる．

その後 1999 年になって Munuera and Ramirez [15] が同じ符号の第 2，第 3 一般化された Hamming 重み[15] を調べる過程でこれらの符号に対する order bound を求めている．それによ

[13] 定義の条件式は $\rho_i + \rho_j = \rho_l$ のミスプリントではない！

[14] 良く知られたことではあるが，[7, Lemma 3.8] に証明をつけておいた．ただし，そこでは $\sqrt{q}, q$ の代わりに q, q^2 を用いている．

[15] $(\mathbf{F}_q)^n$ の部分空間 U について，その重みを

$$\mathrm{wt}\, U = {}^{\#}\{i \in \{1, \ldots, n\} \mid \exists \boldsymbol{u} = (u_1, \ldots, u_n) \in U \text{ s.t. } u_i \neq 0\}$$

で定める．この概念は $\boldsymbol{u} \in (\mathbf{F}_q)^n$ について，$U = <\boldsymbol{u}>$ として考えると定義 2.1 で述べたものに一致する．

$$d_r = \min\{\mathrm{wt}\, U \mid U \subseteq C,\ \dim U = r\}$$

を**第 r 一般化された Hamming 重み**とよぶ．Heijnen and Pellikaan [5] では定理 5.3 を d_1 の場合として含むような形で d_r に対し order bound を定式化している．

れば，$d(C_\Omega(D, mP_\infty))$ について，order bound の与える下界は Yang and Kumar [18] が与えた $d(C_L(D, mP_\infty))$ の真の値から関係 (6) によって計算した真の値に一致していた．

この辺りをもう少し詳しく述べて見る．$P_\infty \in \mathcal{H}_{\sqrt{q}}$ における Weierstrass 半群は $\sqrt{q}$ を法として並べると見やすい:

$$\{a\sqrt{q}+b \mid a,b \in \mathbb{N}_0,\ 0 \le b \le \sqrt{q}-1,\ b \le a\}. \tag{7}$$

また，状況設定 5.1 での M は，この場合 $(q+\sqrt{q}-2)\sqrt{q}+\sqrt{q}-1$ である．さらに，(7) を $\rho_l < M$ で $C_\Omega(D, \rho_l P_\infty) \neq C_\Omega(D, \rho_{l+1} P_\infty)$ なるものだけに制限すると

$$\{a\sqrt{q}+b \mid a,b \in \mathbb{N}_0,\ 0 \le b \le \sqrt{q}-1,\ a-q+1 \le b \le a\} \setminus \{(q+\sqrt{q}-2)\sqrt{q}+\sqrt{q}-1\}. \tag{8}$$

となる．(8) から $a(l)$ を具体的に計算すると次のようになる．

補題 5.6 (7) の元を小さい順に $\rho_1, \rho_2 \ldots$ とし，$\rho_l = a\sqrt{q}+b$ $(0 \le b \le \sqrt{q}-1,\ b \le a)$ と書くと

(i) $0 \le a = b \le \sqrt{q}-2$ のとき，$a(l) = a+2$,

(ii) $0 \le b \le \sqrt{q}-2$ かつ $a-\sqrt{q}-1 \le b < a$ のとき，$a(l) = (a-b)(b+2)$,

(iii) "$0 \le b \le \sqrt{q}-2$ かつ $a-q+1 \le b < a-\sqrt{q}-1$" または "$b = \sqrt{q}-1$ かつ $\sqrt{q}-1 \le a \le q+\sqrt{q}-3$" のとき，$a(l) = (a+1-\sqrt{q})\sqrt{q}+b+2$,

である．

この補題から $b(l)$ を計算することができ，その値が [18] から計算したものと一致する．

6 おわりに

S. J. Kim[13, 1994 年] (および，この仕事にに触発された筆者の [6, 1996 年]) により曲線上の点についての Weierstrass 半群ないし gap 列という概念を 2 点または複数点の場合へ拡張しその性質を調べるという研究が始まった．これにより，曲線上の 2 点符号について調べるという機運が熟し，Matthews [14] があらわれた．これは 2 点符号の場合に定理 4.4 に対応する結果を得たものだった．さらに，S. J. Kim と筆者は [8] で定理 4.5 に対応する結果を得た．その中で，結果の応用として Hermitian 曲線 (5) 上のいくつかの 2 点符号について，その最小距離 $d(C_\Omega(D, mP_\infty + nP_0))$ を評価したところ同じ曲線上の 1 点符号で次元が同じものと比べたとき最小距離が 1 点符号より改善されるものがあることが分かった．

その後われわれは 2 点符号について，1 点符号の場合の [18] に対応する結果を得た [9, 10, 11, 12]．そこでは [18] の手法をさらに込み入った複雑な形に発展させて用いた．$d(C_\Omega(D, mP_\infty + nP_0))$ の系統と $d(C_L(D, mP_\infty + nP_0))$ の系統の間には (6) のような等号ではないが Hamming 距離を保存する同型を構成できるので，もし 2 点符号に対して order bound のようなものが定式化できればわれわれの結果の証明を短くすることが期待できる．最近 Beelen[1] によって 2 点符号にも適用可能な形で d_1 に対する order bound が定式化され，その与える下界はわれわれの結果に広範囲で良くフィットしている．

最後にひとつの問題を提起して，この稿を終わりたい．Garcia-Kim-Lax の評価にあらわれる式，すなわち定理 4.5 での評価式の右辺は $\mathbb{N}_0$ の部分半群 S が与えられれば意味を持つ．(ただし

genus は $\#(\mathbb{N}_0 \setminus S)$ と解釈する．）また，order bound については，$b(l)$ を少しばかり変形した式 $b'(l) = \min\{a(l') \mid \rho_l \leq \rho_{l'}\}$ を考えれば $\mathbb{N}_0$ の部分半群 S に対しても意味を持つ．($a(l)$ の定義は $\rho_l < M$ の条件をはずしても意味を持つ．）これら 2 つの量の間にはどのような関係があるのだろうか？

参考文献

[1] P. Beelen, *The order bound for general algebraic geometric codes*, Finite Fields Appl., 13 (2007), pp. 665–680.

[2] G. -L. Feng and T. R. N. Rao, *Decoding of algebraic geometric codes up to the designed minimum distance*, IEEE Trans. Inform. Theory, 39 (1993), pp. 37–45.

[3] A. Garcia, R. F. Lax, *Goppa codes and Weierstrass gaps*, in: H. Stichtenoth, M. A. Tsfasman (eds.), Coding Theory and Algebraic Geometry, Lecture Note in Mathematics 1518, Springer - Verlag, Berlin - Heidelberg, (1992), pp. 33–42.

[4] A. Garcia, S. J. Kim, R. F. Lax, *Consecutive Weierstrass gaps and minimum distance of Goppa codes*, J. Pure Appl. Algebra 84 (1993), pp. 199–207.

[5] T. Heijnen and R. Pellikaan, *Generalized Hamming weights of q-ary Reed-Muller codes*, IEEE Trans. Inform. Theory, 44 (1998), pp. 181–197.

[6] M. Homma, *The Weierstrass semigroup of a pair of points on a curve*, Arch. Math. 67 (1996), pp. 337–348.

[7] M. Homma, *Galois points for a Hermitian curve*, Comm. Algebra, 34 (2006), pp. 4503–4511.

[8] M. Homma and S. J. Kim, *Goppa codes with Weierstrass pairs*, J. Pure Appl. Algebra 62 (2001), pp. 273–290.

[9] M. Homma and S. J. Kim, *Toward the determination of the minimum distance of two-point codes on a Hermitian curve*, Des. Codes Crypt., 37 (2005), pp. 111–132.

[10] M. Homma and S. J. Kim, *The two-point codes on a Hermitian curve with the designed minimum distance*, Des. Codes Crypt., 38 (2006), pp. 55–81.

[11] M. Homma and S. J. Kim, *The two-point codes with the designed distance on a Hermitian curve in even characteristic*, Des. Codes Crypt., 39 (2006), pp. 375–386.

[12] M. Homma and S. J. Kim, *The complete determination of the minimum distance of two-point codes on a Hermitian curve*, Des. Codes Crypt., 40 (2006), pp. 5–24.

[13] S. J. Kim, *On the index of the Weierstrass semigroup of a pair of points on a curve*, Arch. Math. 62 (1994), pp. 73–82.

[14] G. L. Matthews, *Weierstrass pairs and minimum distance of Goppa codes*, Designs, Codes and Cryptography 22 (2001), 107–121.

[15] C. Munuera and D. Ramirez, *The second and third generalized Hamming weights of Hermitian codes*, IEEE Trans. Inform. Theory, 45 (1999), pp. 709–713.

[16] H. Stichtenoth, Algebraic function fields and codes, Springer-Verlag, Berlin Heidelberg, (1993).

[17] K. Yang, *On the weight hierarchy of Hermitian and other geometric Goppa codes*, Ph. D. Thesis, University of Southern California, (1992).

[18] K. Yang, P. V. Kumar, *On the true minimum distance of Hermitian codes*, in: H. Stichtenoth, M. A. Tsfasman (eds.), Coding Theory and Algebraic Geometry (Luminy, 1991), Lecture Note in Mathematics **1518**, Springer - Verlag, Berlin - Heidelberg, (1992), pp. 99–107.